TOOLS
AND
WEAPONS

The Promise and
the Peril of
the Digital Age

TOOL
WEAPON

工具，还是武器？

直面人类科技最紧迫的
争议性问题

[美] 布拉德·史密斯（Brad Smith）
卡罗尔·安·布朗（Carol Ann Browne） 著
杨静娴 赵磊／译

中信出版集团

当科技悖论挑战全球，
未来在每个人的手中！

亲历世界风云变幻，
披露全球“暗礁”细节，
探索人类未来科技安全边界

微软总裁
扛鼎之作
《纽约时报》畅销图书

比尔·盖茨 × 沈向洋
倾情作序
美国前国务卿等人
联袂推荐

VISIT...

LANZAROTE

Caliente.COM

TOOLS
AND
WEAPONS

The Promise and
the Peril of
the Digital Age

TOOL

WEAPON

工具，还是武器？

直面人类科技最紧迫的争议性问题

当科技悖论挑战全球，
未来在每个人的手中！

亲历世界风云变幻，
披露全球“暗礁”细节，
探索人类未来科技安全边界

微软总裁
扛鼎之作
《纽约时报》畅销图书

比尔·盖茨×沈向洋
倾情作序
美国前国务卿等人
联袂推荐

[美] 布拉德·史密斯（Brad Smith）
卡罗尔·安·布朗（Carol Ann Browne）著
杨静娴 赵磊／译

中信出版集团

版权信息

书名:工具，还是武器？

作者:[美]布拉德·史密斯 [美]卡罗尔·安·布朗

译者:杨静娴 赵磊

出版时间：2020-02-01

ISBN:9787521713169

中信出版集团制作发行

版权所有·侵权必究

谨献给我们的母亲
她们无缘阅读本书
但她们的爱书之情
激励我们成就此作

推荐序一

直面当今科技行业最紧迫的争议性问题

比尔·盖茨
微软创始人

我和布拉德·史密斯相识于我职业生涯最艰难的时刻，那是我第一次向他寻求建议。自那之后，20年过去了，我依然仰仗他的真知灼见。

布拉德于1993年加盟微软的法律团队，但我们直到90年代末才真正熟悉。当时，美国政府正在对微软提起反垄断诉讼，我们夜以继日地并肩工作。我很快发现布拉德成熟老练并长于思考，因此我不仅越来越敬重他的为人，也越来越依赖他的专业判断。

在应对反垄断诉讼的过程中，布拉德制定了我们的法律策略。不仅如此，他还做出了一些重要性丝毫不输前者的贡献：推动公司在文化和战略层面进行重大转型。这种转型构成了这本书的核心。

在微软发展的早期，我们很少花时间与联邦政府的官员进行沟通，而我颇以此为豪。我总是告诉人们："虽然我们在华盛顿特区连一间办公室也没有，但我们成功了，这难道不是一件了不起的事吗？"然而，在反垄断诉讼案的应诉过程中，我痛苦地认识到，之前的做法并不是明智之举。

诉讼案和解之后，布拉德说服了我和微软内部许多人，让我们认识到需要改变策略，还为我们指明了应如何做到这一切。布拉德是一名律师，不是软件开发程序员。尽管他精通技术，但他和其他人思考问题的方式并不完全一样（我这么说绝对是真心赞赏）。他意识到，我们需要投入更多的时间和精力与各方建立广泛的联系，包括政府、我们的合作伙伴，甚至我们的竞争对手。如果布拉德投身外交界，一定可以成为一名伟大的外交官。鉴于他早年对国际关系非常感兴趣，这么说并不为过。

布拉德的一个特点是，不仅从微软的利益出发考虑问题，还充分认识到科技以及会对科技产生影响的政策的重要性。因此，他认为，远离政治不仅是我们一家公司犯下的错误，也是整个行业犯下的错误。尽管有时候我们需要独自面对风险，但在涉及人工智能、人脸识别和网络安全时，整个行

业携手合作会带来更大的收获。

正如他在这本书中所论述的那样，政府采取更严格的监管措施有时候确实符合每个人的利益（当然，布拉德也清醒地意识到，自己作为一位商界领袖呼吁政府制定更多的法规而非减少法规监管，略具讽刺）。为此，他希望微软和其他科技公司更多地与美国、欧洲及其他地区的领导人接触。我因我们在华盛顿没有办公室而扬扬自得的时代已经一去不复返了。

布拉德的观点从未像今天这样与我们息息相关。目前，全球各国政府正在严格审视许多科技公司，乃至整个科技行业。它们如何应用科技？科技会造成什么影响？科技公司应承担什么责任？政府以及全社会又应该如何看待这些问题？

尽管这些问题与我们20年前面对的问题不尽相同，但布拉德当时的见解在今天依然极具价值。

以人脸识别技术带来的问题为例，尽管这个话题尚未引发巨大的公众争论，但它在未来一定会引发众议。软件公司应该如何限制人们对人脸识别工具的使用？行业应该如何看待这一点，以及什么样的政策法规才是有意义的？

布拉德一直引领着对相关问题的思考，并广泛建立伙伴关系对其加以探讨。科技行业需要团结一致，并与全球各地的客户和政府通力合作。我们也许不能吸引所有人参与其中，但如果我们任由各方各行其是，并因此导致不同国家各自为政地制定法规，那么无论是对客户、科技行业，还是对整个社会来说，都绝非善事。

这本书探讨了15个发人深省的问题，其中包括网络安全、信息技术从业者的多样性和中美关系等问题。如果我必须从中挑选出最重要的一个章节，我会选择关于隐私的章节。收集海量数据的能力是一把双刃剑：一方面，它使政府、企业和个人能够做出更好的决策；另一方面，它也带来了一个大问题，即我们如何能够在使用这些数据的同时保护人们的隐私。

然而，正如布拉德所说，尽管相关技术相对新兴，但其引发的问题并不新鲜。几个世纪以来，人们一直在与该问题的这个或那个版本做斗争。尽管你可能会想到，数据隐私那一章会谈到纳粹德国收集本国人民信息的方式，但你应该不会料到它还提及了1812年的战争，甚至简单介绍了《司法互助条约》的历史。

这既显示了布拉德涉猎广泛，也凸显了他深入研究问题的能力。同时，这些内容绝不像枯燥乏味的法律简报。布拉德和这本书的合著者卡罗尔·安·

布朗擅长把故事讲得引人入胜，从局内人的视角生动地描述这些问题如何在全球各地的会议室和法庭被反复探讨。布拉德不仅仅是坐下来独自分析事物，还把人们聚集在一起寻找解决方案。

布拉德和我一直通过面谈和邮件保持密切联系，并就这些问题进行交流。直至今日，我仍无比倚赖他的智慧与判断力。鉴于他的经验和睿智，他是指引我们深入思考当今科技行业面临的问题的最佳人选。

目前，这些问题的重要性正在与日俱增。这本书提供了一个清晰的视角，帮助我们审视科技引发的一系列问题，并为科技公司和社会指出一条可能的前进道路。可以说，布拉德针对当今科技行业最紧迫的一些争议性问题，为我们奉上了一本清晰和令人信服的指南。

2019年4月

推荐序二

天下之器，驭之以道

沈向洋
微软全球执行副总裁，
微软人工智能及微软研究事业部负责人

布拉德·史密斯和我都是在20世纪90年代加入微软的老兵。毫无疑问，布拉德代表了我头脑中一位杰出律师应有的样子：严谨、睿智、博古通今、无所不知。让我觉得最难能可贵的是，他还像我们这些搞技术的家伙一样，时刻关注科学技术的发展和创新，并且始终保持一颗探究到底的好奇心。

在每周的微软高级管理团队例会中，我最喜欢与布拉德一起探讨问题。尽管他是微软的头牌大律师，而我是一个搞技术、做研究的“书呆子”，但我们之间却从来不缺少共同的话题，从数据隐私、网络安全、人才培养，到我们发展、应用、普及人工智能的目的、准则，以及我们应当肩负的社会责任。虽然我们的出发点各有侧重，但在技术发展之于人类社会、法律法规、道德伦理的思考上，却常常能产生共鸣。

2018年，布拉德和我将我们对于人工智能发展过程中可能引发的道德、法律思考和社会影响的讨论，汇编成《计算未来：人工智能及其社会角色》一书，并在书中阐述了微软人工智能的6项原则：公平、可靠和安全、隐私和保障、包容、透明、责任。我们希望能让更多的人认识、理解和参与我们对于人工智能和人类社会未来发展的思考及探讨。

布拉德与卡罗尔合著的新书《工具，还是武器？》开门见山地提出了一个备受关注的问题——就像炸药与原子能的发明一样，技术创新的成果，究竟是成为用以帮助、增强、改善、提高的工具，还是用来伤害和毁灭的武器。这中间的差异，不仅仅是一词之差，更是永远摆在科技界乃至整个社会面前的挑战。

身为技术创新的推动者，我尤其深切地感受到，我们有责任确保技术走向正确的方向。通过几十年的观察，我注意到新技术的发展和应用常常并不是一条简单的直线，更多的时候会呈现出一个周而复始的循环：首先，科学家做出一项科技创新；其次，技术在产品化的过程中，得到普及和应

用；应用的次数越多，想的内容也就越多，人们开始回过头审视暴露的问题，并且开始反思，我们该如何更好、更安全、更高效地利用这项技术。

汽车安全带普及的过程最具代表性。20世纪初，汽车迅速在美国社会得到普及，但交通法规的制定和完善，却拖拖拉拉地持续了几十年。1968年，美国法律第一次要求汽车必须配备安全带，但真正强制要求司机扣好安全带的法规，直到1984年才出台。试想，如果人们能早几十年意识到安全带的重要性，是不是会挽救成千上万条生命。

今天，以人工智能为代表的新一代数字技术，取得了前所未有的快速发展。语音、视觉、语言、阅读、翻译，在人工智能研究的各个领域里，都在快速接近人类水平。与此同时，我们也注意到，人工智能应用场景的多样化发展，也带来了人们对于隐私、歧视、安全等问题的担忧和思考。作为技术创新的引领者，我们在推动技术进步的同时，更应该认真思考可能由此带来的社会影响，以及人类将要共同面对的潜在挑战，未雨绸缪，防患于未然，从头开始打造负责任的人工智能。

就像布拉德在书中所说，像20年前的微软一样，今天的科技行业必须认识到一个基本且至关重要的原则——如果你掌握了能够改变世界的科技，那么你就有责任帮助解决你创造的世界所面临的问题。

在《工具，还是武器？》一书中，布拉德以他所擅长的严谨的叙事，将微软乃至整个科技产业，对于数据隐私、网络安全、社交媒体、数字外交、人才培养、社会责任，甚至国际合作等话题的全面思考娓娓道来，既向人们展示了技术发展为全球经济带来的发展机会，也毫不掩饰地指出了在社会、法律、道德层面急需解决的种种隐患和问题。

今天，人工智能正在开启一个从技术创新到普及，再到责任的全新发展循环，而我们要做的，就是驭之以道、律之以法、束之以德，携手把握未来趋势，引领智能互联网的发展，为全人类创造一个更加美好的未来。打造负责任的、可信赖的人工智能，不仅是我们的愿景，更是我们共同的责任。毕竟，我们谁也不希望等到几十年后，才为人工智能补上一根迟到的“安全带”。

2019年12月18日

序言

云：全世界的文件柜

文明的演进一直依赖数据。

人类的历史始于人开始具备交谈能力之时。随着语言的出现，人们得以分享彼此的想法、经历，以及欲望与需求。

随着人类逐步拥有书写能力，文明的进步也开始加速。从此，思想不仅能够在人与人之间口口相传，还能够更容易和更准确地传播到不同地方。

新的火花随之出现，并点燃了知识的火苗，这就是存储、检索和分享人类成文内容的能力。古代世界的重要标志之一就是图书馆的诞生[注]。保存下来的文件和图书意味着人们不仅能够更容易地跨越空间进行交流，还能够跨越时间，将信息代代相传。15世纪，谷登堡发明了铅活字印刷。从此，火苗变成了熊熊火焰，赋予作者和读者更大的能量和空间。

这场知识的烈焰最终席卷全世界。在随后的几百年间，商业呈现爆炸式增长，而这既成为交流增加的原因，也是交流增加的结果。当初，每间办公室都需要一个存储文件的设备，房间被文件柜占据[注]。

毋庸讳言，数据自出现以来一直在人类社会中占据重要的地位，但它的重要性从未像今天这样凸显。即使在贸易放缓或经济衰退时期，数据仍然会以稳定的速度增长。有人说，数据已经成为21世纪的“石油”。这种说法并不足以说明数据的重要性。一个世纪前，汽车、飞机和火车需要依靠石油开动，而在今天，人类生活的方方面面都是由数据驱动的。可以说，在现代文明中，数据更像是我们呼吸的空气，而不是我们使用的石油。

与石油不同，数据已经成为一种可再生资源，并由我们人类自己创造。预计到2020年底，数字数据量将达到2010年的25倍[注]。借助人工智能，即AI，我们对数据的应用已经达到前所未有的程度。

我们将支持这种应用的数字基础设施称为“云”。虽然这个名字听起来柔软蓬松，但“云”实际上是一个堡垒。每次你在智能手机上进行浏览，其实都会从一个庞大的数据中心提取数据，而数据中心是一个常人难以进入的现代奇迹。

如果你有机会参观一个数据中心，你会更好地了解当今世界是如何运转的。

了解云到底是如何运作的最佳地点之一，位于西雅图以东约150英里、90号州际公路旁的华盛顿州小城昆西。昆西的地理位置得天独厚，地处华盛顿州以农业为主的盆地中心，背靠由美国西部最大的水道哥伦比亚河冲刷数千年所形成的一个陡峭峡谷。这个小城坐享充沛的水电网络供电，包括美国最大的水电站大古力水坝。对于现代数据中心这个已成为当今世界最耗电的设施而言，这是一个理想的环境。

在昆西主街几个街区开外的地方，你会发现多座不起眼的建筑，受到高高的栅栏和高墙的严密保护。其中一些建筑上有某家科技公司的标识，一些则完全没有标识。这些建筑中最大的一个被称为哥伦比亚数据中心，为微软所有。

对于一个数据中心而言，它仅从规模来看就是一个令人兴奋的存在，甚至有一些令人望而生畏。我们在昆西的设施不只是一座单独的建筑物，而是由20多栋建筑组成的两个数据中心园区，总面积达200万平方英尺。每栋建筑都有两个足球场大小，足够停放两架大型商用飞机。这个建筑群中摆放着数十万台计算机服务器和数百万块硬盘，它们每三年更新一次，换成速度更快、效率更高的型号。

如果想全面感受数据中心的规模，最好的方法是从其最外部走到中心。每栋大楼的墙外都安放着世界上最大的发电机，随时准备在几秒钟内启动发电，确保数据中心在本地电网停止供电时不会出现任何中断。每台发电机的高度都超过20英尺，发电量相当于可供2000多户家庭使用的电力。这些发电机与柴油燃料箱相连，其燃料能够确保数据中心在停电48小时内正常运行。同时，我们还制订了相关的加油预案，以便在必要时保证长期发电。在新建的数据中心，如怀俄明州夏延地区的设施中，发电机使用更为清洁的天然气，并为当地电网提供备用电源。几十台这样的大型发电机放置在数据中心大楼旁随时待命，万一大古力水坝的水电出问题，这些发电机可以提供电力。

在每栋大楼内部，都有一连串大型安全室作为变电室运行，它们通常从电网中输入23万伏的电力，然后将其变电到240伏，供数据中心的计算机使用。这些变电室内排列着多个6英尺长的机架，每个机架连接着500块或更多数量的电池，看起来和你掀开引擎盖后看到的情况一样。房间的每扇门都防弹，所有墙壁也防火，防止火灾从一个房间蔓延到另一个房间。一个典型的数据中心建筑内会有4个或更多这样的房间，根据配置，最多可容

纳5000块电池。这些电池有两个用途。首先，来自电网的电流通过机架，保持电池充电，并消除潜在的电流尖峰，从而使流向计算机的电流保持平稳恒定。其次，在停电的情况下，电池将保持数据中心的运行，直到发电机启动。

通过另一串防弹门和防火墙，你会看到另一个由两个穿制服的警卫负责操作的，像是机场安检用的金属探测器立在你和大楼的内部密室之间。只有那些位列预先批准名单上的全职微软员工才能进入内部。首先，你需要进入一间小小的接待室，一扇铁门在你身后徐徐关上，将你锁在室内，安保人员会通过摄像头将你里里外外检查完毕，然后才会打开下一扇防弹门。

最后，你将进入一个洞穴般的房间，一座通向信息时代的神殿，我们数字生活的基石。一阵低沉的嗡嗡声欢迎你进入数据神经中枢，它由摆满一排排计算机的落地式机架组成，一直延伸到你的视线之外。这个庞大的钢铁和电路库包括大小相同的多台服务器，每台服务器均存储着各自独特的海量数据。它们就是数字世界的文件柜。

在这些建筑物内的某个房间里，也许就存储着属于你的数据文件，包括你今天早上新写的电子邮件、昨晚撰写的文档，以及昨天下午拍摄的照片，还可能包括你提供给银行、医生和雇主的个人信息。这些文件只占这座设施内成千上万台计算机中的某个硬盘的一小部分。每个文件都是加密的，即所有信息均已进行编码，只有该数据的授权用户才能读取。

每个数据中心的大楼都有多个类似的房间，彼此相互隔离，以保证在发生火灾时的安全。每套计算机都与大楼内的三个电源相连接。同时每一排都被设计成在整个建筑内循环利用电脑散发的热量，以减少冬季的供暖和用电需求。

当你离开服务器机房时，你将再次通过严格的安全检查。你需要脱掉鞋子，解下皮带。你可能认为，事实上，你在离开机场时都不必忍受这样的检查，此时你的向导会提醒你，进出都进行安全检查自有其道理。微软希望确保没有人会使用U盘复制数据，或窃取存储着某人个人数据的硬盘。此外，当硬盘需要更换时，它们的数据将被复制到新的硬盘上，原来的文件将被删除。然后，废弃的硬盘会通过类似碎纸机的巨大机器被彻底销毁。

从某种意义上讲，最值得一提的特性要留到参观结束之时才会被揭示。你的向导会解释说，每个数据中心都有另一组同样的备份设施，以便企业、政府或非营利组织的数据能够得到不间断备份。这样，如果发生地震、飓风或其他自然灾害或人为灾难，将及时切换到备份数据中心，以保持云服务的平稳运行。例如，当日本北部发生地震时，我们在日本南部设立的备

份数据中心就确保我们的服务不会中断。

如今，微软在20多个国家或地区的100多个地点拥有、运营和租赁了不同规模的数据中心（这一数字还在不断增长），提供200种在线服务，并为140多个市场中超过10亿的客户提供支持。

当我于1993年加入微软时，开办一家软件公司并不需要多少资金。我们的两位联合创始人比尔·盖茨和保罗·艾伦的创业故事与许多技术开发人员的创业经历别无二致，他们都在车库或大学宿舍创办了自己的公司。这其中关键的一点是开发软件并不需要多少投资，只需一台好电脑，一个小小的储蓄账户，以及一份愿意以快餐果腹的坚定信念，就足以起步。

在微软从一家小小的初创企业成长为巨型跨国公司的历程中，我们一次又一次地见证了这一点。2004年，我们希望收购一家名为“巨人软件公司”（Giant Company Software）的反间谍软件公司。我们的团队通过其公开发布的技术支持电话联系到了它的员工，当微软的工作人员要求将电话转接给它的首席执行官时，电话那一端的听筒似乎只是简单地被递给了坐在对面的那位雇员。毫不奇怪，我们的收购谈判进展迅速注。

我在参观我们的一个数据中心时，不由自主地想到了巨人软件公司。你现在仍然可以像比尔和保罗当年创业一样开发一个新的应用程序，无数开源软件开发人员也一直在这样做，但是在全球范围内提供云计算所需的平台则是另一回事。当我在成千上万台闪烁的电脑、成排的电池和巨大的发电机之间行走时，我感觉进入了一个不同的时代，甚至好像登上了另一个星球。数据中心园区的建设成本高达数亿美元，而施工结束后，设施维护和升级的工作将立即开始。设施需要扩展，服务器、硬盘和电池需要不断更新换代为更新、更高效的型号。可以说，一个数据中心永无完工之日。

在许多方面，现代化的数据中心位于我们已经进入的新数字时代的核心。其积累的数据、存储和计算能力为推动世界经济的发展提供了一个前所未有的平台，也引发了我们这个时代许多极具挑战性的问题。在这个新的时代，我们应如何在公共安全、个人便利和个人隐私之间达到恰当的平衡？我们又应如何保护自己免受网络攻击，这些攻击正在利用信息技术破坏国家、企业或个人的生活？我们应如何管理其对整个社会经济的影响？我们正在创造的世界是否能够为我们的孩子提供充分的就业机会？我们是否正在创造一个我们能够控制的世界？

要获得上述问题的答案，我们首先需要更好地理解科技是如何演进的，而科技在过去的发展历程可以部分地帮助我们实现这种理解。

自古以来，任何工具都是既可助人，也可伤人。即便一把扫帚，也是如

此，它既能被用来扫地，也能被用来打人。一件工具的功能越强大，其所带来的益处或伤害就越大。尽管全面的数字化转型为世界带来了机遇，但信息技术无疑既已被打造成为一个强大的工具，也已日益成为一个杀伤力巨大的武器。

这一新兴的技术时代已渐渐将我们带入一个焦虑的新时代，这种紧张关系在各民主国家中尤为明显。因移民、贸易和收入不平等问题引发的不安使这些国家日益面临民粹主义和民族主义的裂痕，造成这种情况的部分原因正是影响深远的科技转型。科技带来的益处并未均匀地分配，同时变革的性质和速度对个人、社区与整个国家都提出了挑战。民主社会共同面临近一个世纪以来最大的挑战，同时在某些情况下，还有一些国家则正在利用科技为自己谋求私利。

本书从全球科技巨头掌舵者的角度探讨了上述问题。它讲述了科技行业正如何努力与诸多强大的力量达成共识，这些力量远远比任何一家科技公司，乃至整个行业都更为强大。同时本书不仅讲述了趋势和策略，还讲述了为应对快速变化的世界，许多有关人、决策与行动的故事。

这是一出正在上演的大戏，作为微软的一员，我们有时会从不同的角度观看它。20年前，我们被推入一个旋涡的中心，它可以被视作现代信息技术与世界的第一次碰撞。美国司法部和20个州共同提起了一场针对微软的反垄断诉讼，试图拆分微软，其他国家的政府也紧随其后。竞争事务官员们一致认为，因为Windows操作系统太重要了，因此不能任由它不受监管。

虽然我们成功地保护了公司免于解体，但那仍然是一个艰难和充满挫败的痛苦经历。2002年，我被任命为公司的总法律顾问，我的工作就是与世界各国政府和业内同人敲定类似的友好协议。为此，我们花了将近10年的时间[注]，并且犯下了很多不该犯的错误。鉴于我的角色，我在某种程度上对几乎所有错误都难辞其咎。

好在我们成功应对了挑战，并变得更加成熟和明智。我们知道，我们需要时常照镜子，并从中看到别人眼中的我们，而不仅仅是我们自己希望看到的模样。微软就好像是一所新学校的首届毕业班的一员，也许不在排名第一的班级，但我们的优势是先于其他人完成了学业。

与20年前相比，今天，人们面临的科技问题更为广泛和深入。我们已经到达科技和社会的一个关键转折点。这是一个充满机遇的时刻，同时也需要立即行动，解决紧迫的问题。

因此，像20年前的微软一样，科技行业需要做出改变。我们必须认识到一个基本且至关重要的原则：如果你掌握了能够改变世界的科技，那么你就

有责任帮助解决你所创造的世界面临的问题。这听上去似乎无可争议，但鉴于科技行业长期专注快速成长，有时甚至将颠覆作为自身发展的目标，坚持这一原则就不那么简单了。简而言之，创造科技的公司必须承担更大的责任。

不过，也不能忘记另一个同样重要的原则——科技行业不能独自应对这些挑战。世界需要一个自律与政府监管相结合的解决方案。这同样也对各个国家带来了更大的冲击，部分原因是，在技术具有如此大的破坏力的今天，这些国家更加依赖广泛的经济和社会共识。现在，唤起许多政府行动的意愿似乎比以往更难，但已经刻不容缓，政府必须制定新的政策和计划（无论是独立行动，还是相互协作），并需要以新的形式与科技行业进行合作。简而言之，政府需要加快速度，尽快跟上科技发展的步伐。

这些挑战并无先例可循，不过我们仍然可以从过去学到许多经验教训，进而为今日所用。自18世纪中叶，第一次工业革命在英格兰中部地区爆发以来，技术变革已经多次席卷世界各地。对于今天面临的每一个看似前所未有的挑战，我们通常都能在历史上找到参照，虽然具体情况不同，但能够帮助我们更好地洞察今天面临的挑战。本书以史为鉴，就我们可以如何吸取过去的教训进行了思考，并对未来的机遇和挑战进行了探讨。

最终，这些问题涉及技术及其对我们的工作、安全以及世界上最基本的人权的影响。在当今这个技术快速变革的时代，我们需要将其与传统乃至永恒不变的价值观相协调。为了实现这一目标，我们既要确保持续创新，又要确保技术变革的方式能够让技术以及创造技术的公司受到应有的约束，从而满足社会和我们共同定义自身命运的需要。

---

1. 世界上最早的档案数据如果放在现代数据中心，也丝毫不显突兀。例如，考古学家在叙利亚的埃布拉古国发现了一个皇家档案馆的遗迹，该档案馆在公元前2300年左右被摧毁。除了苏美尔神话的文本和宫廷书记们使用的其他文件外，还有2000块写满行政管理档案的泥板，其中包含了有关纺织品和金属，以及谷物、橄榄油、土地和动物分配的详细信息。Lionel Casson，*Libraries in the Ancient World* (New Haven, CT: Yale University Press, 2001)，3–4。一个当代数据分析团队在我们这个时代使用类似的数据集，也并非一个难以想象的场景。在接下来的几个世纪里，图书馆遍布古地中海地区，先是在繁荣的希腊城邦，再传到亚历山大港，最后到了罗马。随着人类发展出语言能力，并能够在莎草纸卷轴而非泥板上储存文字，这些图书馆的收藏也变得多种多样。古亚历山大图书馆建于公元前300年左右，曾经藏有49万卷文献。Casson，*Libraries*,36。与此同时，在东

亚，私人图书馆如雨后春笋般涌现，典籍都记录在简牍上。中国人发明了造纸术，这是一个重大的突破，它“使东方领先于西方几个世纪，使精细的管理和官僚制度得以建立”。James W.P.Campbell,*The Library: A World History* (Chicago: The University of Chicago Press, 2013),95。

2. 有关文件柜的发明的逸事说明了数据存储需求随着时间推移而发生的变化。1898年，美国保险代理人埃德温·西贝尔对当时的数据存放方法日益感到不满。西贝尔住在南卡罗来纳州，为棉农提供保险。那里的棉花采摘完毕后，将横跨大西洋运往欧洲的纺织厂。这份工作涉及大量需要妥善保管的文书。在西贝尔的时代，企业将记录归档进靠墙堆放在地板到天花板的木制“鸽子洞”里。纸张通常被折叠起来，塞进信封里，然后塞进小盒子里，通常需要爬上梯子才能够到。这不是一种简单或有效的存储信息的方法，特别是如果你不确定文件到底存放在哪里而不得不到处搜寻它。

   像任何一个优秀的发明家一样，西贝尔看到了一个需要解决的问题，随后想出了一个简单而聪明的主意：一个由木制盒子组成的垂直文件存放系统。他与辛辛那提的一家制造商合作，做出了5个带抽屉的盒子，抽屉里可以存放竖立的文件，从而使办事员无须打开信封就可以快速翻阅和查找文件。后来，文件还会被插进文件夹，并且中间由标签隔开。于是，现代文件柜就此诞生了。James Ward,*The Perfection of the Paper Clip: Curious Tales of Invention, Accidental Genius, and Stationery Obsession* (New York: Atria Books, 2015),255– 56。

3. David Reinsel, John Gantz, and John Rydning,*Data Age 2025: The Digitization of the World From Edge to Core* (IDC White Paper–#US44413318,Sponsored by Seagate)November 2018，6，https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

4. 1英里≈1609米。

5. João Marques Lima, “Data centres of the world will consume 1/5 of Earth’s power by 2025,” Data Economy, December 12, 2017, https://data-economy.com/data-centres-world-will-consume-1-5-earths-power-2025/.

6. 1平方英尺≈0.09平方米。

7. 1英尺≈0.3米。

8. Ryan Naraine, “Microsoft Makes Giant Anti-Spyware Acquisition,”

eWEEK,December 16，2004，http://www.eweek.com/news/microsoft-makes-giantanti-spyware-acquisition.

9. 微软这场反垄断大戏带来许多启示，包括如果一家公司未能解决引起政府当局关注的问题，那么其面临的审查和执法时间将长到令人难以置信。21世纪初，微软解决了其在美国的问题，但直到2009年12月，公司才在布鲁塞尔与欧盟委员会达成最终的主要协议。European Commission, “Antitrust: Commission Accepts Microsoft Commitments to Give Users Browser Choice,” December 16，2019，http://europa.eu/rapid/press-release_ IP-09-1941_en.htm。从开始到最终结束，对微软的众多调查和诉讼几乎持续了30年。公司的反垄断问题始于1990年6月，当时联邦贸易委员会对Windows操作系统的营销、许可和分销做法进行了一次得到媒体广泛报道的审查。Andrew I.Gavil and Harry First，*The Microsoft Antitrust Cases: Competition Policy for the Twenty- First Century* (Cambridge, MA: The MIT Press, 2014)。这些诉讼案件历经许多波折，28年后，最后一宗诉讼终于在2018年12月21日和解。从某种意义上说，这是第一次真正的全球反垄断争议，涉及27个国家的调查和诉讼，反映了这一争议的广泛性，最后的案件是加拿大魁北克、安大略和不列颠哥伦比亚省的消费者集体诉讼案。

对于一项科技政策问题而言，30年乍一看似乎极其漫长，但从许多方面来看，在许多重大反垄断问题的处理上，这一时间跨度实属寻常，并不像大多数人想象的那样。1999年，微软正处于其最大诉讼案的阵痛中，我认真研究了20世纪的几场重大反垄断战争，想看看那些公司及其首席执行官如何解决这一问题。这些公司包括标准石油公司、美国钢铁公司、IBM公司和AT＆T公司，它们都定义了当时的领先技术。美国政府于1913年首次针对AT＆T提起反垄断诉讼，尽管在重大的诉讼之间有暂时的喘息之机，但直到1982年，AT＆T同意分拆以解决针对该公司的第三次重大反垄断诉讼，这一问题才最终得到解决。同样，IBM在1932年即与政府在第一次重大反垄断诉讼中对质，但直到它在1984年与欧盟委员会就一项重大诉讼达成和解，关于其主机主导地位的争议方告一段落。又过了10年，IBM大型机主导地位的争议才终于平息，公司终于可以请求华盛顿特区和布鲁塞尔当局结束对其和解方案的监督。Tom Buerkle, “IBM Moves to Defend Mainframe Business in EU,” New York Times,1994年7月8日，https://www.nytimes.com/1994/07/08/business/ worldbusiness/IHT-ibm-move-to- defend-mainframe- business-in-eu.html。这些斗争漫长的持续时间给了我一个教训，使我思考科技公司需要如何应对反垄断和其他监管问题。这

让我在当时得出结论，成功的科技公司需要制定一个积极主动的方针，与当局接触，加强彼此的关系，并最终与政府达成更稳定的协议安排。

第一章
监听项目：三小时起爆的引信

2013年6月6日，初夏的阳光穿透云层洒向大地，在华盛顿州的雷德蒙德，多米尼克·卡尔将他位于微软办公大楼5层的办公室的百叶窗拉开了一些。虽然夏天至少还要一个月才会降临这座位于太平洋西北部的城市，但阳光洒进窗内，带来一丝令人期待的温暖气息，预示着夏天即将到来，繁忙的工作也将稍稍放缓节奏。

他抓起自己的手机朝电梯走去，准备去隔壁的咖啡厅买一个三明治。当他快步走在建筑物之间繁忙的小径上时，他放在衣袋里的手机突然叮了一声。多米尼克向我汇报，他领导着微软的公共事务与沟通团队，负责处理公司与媒体相关最棘手的问题。他总是随身带着手机，而且很少会离开自己的办公桌。

他的手机屏幕亮了起来，显示他收到一封主题为“微软/棱镜”的新电子邮件。当时，我们用“棱镜”代指公司销售团队领导的年度会议，是微软日常业务的一种常规交流。

那封邮件并不是一封常规的业务邮件，而是一个三小时起爆的引信，即将引爆一颗震惊全球的炸弹。“我们写信通知贵司，《卫报》准备于今晚发表一篇关于‘棱镜’计划的文章，该计划是美国几家大型科技公司与美国国家安全局自愿合作的一个秘密计划。”邮件开门见山地点出了美国国家安全局。

这封邮件的发件人也叫多米尼克，全称多米尼克·拉什，是英国著名日报《卫报》的记者。邮件最初发给了微软波士顿办公室的一位公关经理，后者立即转发，并加上了一个被我们称为“红色霹雳”，即红色感叹号的标签，意味着“你需要立即看看这个”。

邮件中有一个复杂的9点内容清单，要求我们答复，并规定了一个不可能的最后期限。拉什解释说：“作为负责任的记者，我们希望给予贵司机会指出上述内容可能包含的任何具体错误……我们已经就此事联系过白宫。鉴于该计划的敏感性，我们只能在第一时间联系贵司寻求答复。”他希望在美国东部夏令时下午6点，或西雅图时间下午3点之前得到答复。

《卫报》获得了机密情报文件，详细说明9家美国科技公司——微软、雅

虎、谷歌、脸书、Paltalk、YouTube、Skype、美国在线和苹果——据称已自愿加入一个名为“棱镜”的计划，允许美国国家安全局直接访问其用户的电子邮件、聊天记录、视频、照片、社交网络详细信息和其他数据。

多米尼克的午餐计划——以及未来一段时间内的大部分计划——都彻底泡汤了。他立刻掉头，两步一个台阶地跑上了5楼。他怀疑这个事件与《卫报》当天早上发表的另一篇令人不安的文章有关。该报已经发表一篇文章，指出据一项秘密的法庭指令，美国电信巨头威瑞森需要“每天持续不断地”向政府提供其美国境内以及美国与其他国家间的通话记录注。这些记录将交由美国国家安全局进行分析，后者的总部位于马里兰州米德堡，长期负责在全球范围内收集信号情报和数据。根据文章，这些批量情报搜集同样针对数百万美国人，而不管他们是否有过任何不当行为。

如果说微软有谁可能知道“棱镜”计划，那一定是约翰·弗兰克，他是公司的律师，领导着公司的法律团队，负责与我们的国家安全相关的工作。多米尼克立刻来到约翰的办公室。

约翰是一个小心谨慎、有条不紊的人，慢慢地消化了多米尼克手机上的《卫报》的信息后，摘下眼镜，从办公桌上挺起身来，凝视着阳光灿烂的窗外，看起来突然疲态尽显。“这完全没有意义，听上去根本不对。”

约翰清楚地知道公司面对执法部门提出的要求具体审查什么内容，以什么方式进行审查。事实上，他参与设计了整套流程。微软只会针对有效的法律程序披露数据，并且只会针对特定的账户或个人。

当约翰和多米尼克来到我的办公室门口时，他们除了那封记者发的邮件之外，几乎没有更多的信息可以提供。约翰说：“如果他们确实做了这种事，那也是在我们完全不知情的情况下。”

没错，我们确实有义务根据法律对用户数据请求进行审查和回应。我们拥有一个既定的程序来仔细审查和回应来自执法部门的所有数据请求。不过微软是一家大公司，这会是某个雇员的恶意行为吗？

我们很快就否定了这个推测。我们很清楚我们的工程体系以及接收、审查和回应政府要求的流程。《卫报》的文章内容与此完全不符。

微软内部没有人听说过“棱镜”计划。《卫报》也不愿意透露它的文章依据的泄密文件。我们设法联系了我们在白宫的熟人，但他们同样不愿意谈论或分享任何“保密”信息。经过一个下午的努力后，我沉思片刻对约翰和多米尼克说道：“也许我们是某个秘密俱乐部的成员，而这个俱乐部实在太隐秘了，连我们自己都不知情。”

我们甚至不得不先等到报道发表，然后才能够开始做出回应。

太平洋夏令时下午3点，《卫报》引爆了它的炸弹：“美国国家安全局‘棱镜’计划利用了苹果、谷歌和其他公司的用户数据[注]。”我们终于知道，所谓“棱镜”，即美国国家安全局的国家安全电子监听计划，其实是资源整合、同步和管理计划工具的缩写[注]。真不知是谁想出了这么一个拗口的名字，这听上去像是科技行业的一个糟糕产品的名称。据新闻媒体报道，这是一个电子监听计划，可以追踪移动设备、电话、电子邮件、在线对话、照片和视频[注]。

几小时之内，《卫报》的文章和《华盛顿邮报》的一篇类似报道传遍全球。我们的销售团队和律师被客户的电话淹没了。

他们都在问同样的问题：“这是真的吗？”

爆料者：爱德华·斯诺登

起初，人们并不清楚媒体是从哪里获取这些信息的，并激烈争论这些信息是否合法。三天后，《卫报》再次释放了一枚重磅炸弹，其冲击力不亚于最初的报道，媒体根据爆料人自己的要求披露了消息来源[注]。

爆料者是美国国防承包商博思艾伦咨询公司一位29岁的雇员，名叫爱德华·斯诺登。他在夏威夷的美国国家安全局威胁行动中心工作，担任合同制计算机系统管理员。他秘密下载了超过100万份高度机密的文件[注]，于2013年5月20日登上飞往香港的航班，在那里与《卫报》和《华盛顿邮报》的记者取得联系，并开始与全世界分享美国国家安全局的秘密[注]。

斯诺登的文件在当年夏天和秋天就变成一系列新闻报道。他泄露的首份文件是一份41页的机密幻灯片演示文稿，用于培训情报人员。这只是一个引子。随后，记者们持续炒作斯诺登藏匿的秘密文件，定期制造头条新闻并持续引发公众焦虑，这个浪潮一直持续到来年。对美国和英国政府搜集电话记录和用户数据（包括外国领导人和数百万无辜美国人的信息）的指责甚嚣尘上，并引发公众对政府一场不信任的海啸[注]。

不出所料，这些消息极大地刺激了公众的神经，因为它们与隐私保护的原则彻底背离，而200多年来，民主社会一直将后者视为理所当然的权利。这些权利正是我们今天在昆西数据中心保护你的信息时所依赖的，它诞生于18世纪伦敦街头的一场激烈争论。点燃这场政治风暴的人是一位国会议

员，名叫约翰·威尔克斯。

约翰·威尔克斯可以说是他那个时代最具戏剧性和最激进的政治家。18世纪60年代，他挑战的对象不仅仅是首相，还包括国王，其语言如此犀利大胆，甚至足以令当今一些政客（几乎会）脸红。1763年4月，威尔克斯在一本反政府期刊上匿名发表了一篇评论。这篇文章激怒了当时的英国总检察长查尔斯·约克，他怀疑文章的作者是威尔克斯，于是英国政府迅速发布了一份搜查令，搜查范围极其广泛，令治安官有权随时搜查几乎任何地方。

他们根据捕风捉影的消息，在半夜闯进一个受到怀疑的印刷商的家中，“把他从妻子身边拖下床，没收了他所有的私人文件，并逮捕了14名工人和仆人”[注]。英国当局随后又迅速搜查了另外4所房屋，共逮捕了49人——几乎所有人都是无辜的公民。他们破门而入，洗劫箱子，并暴力打开了数百把锁[注]。最终，他们根据可靠情报抓住了他们想抓的人——约翰·威尔克斯。

威尔克斯可不是一个轻易服输的人。不到一个月，他就提起了十几起诉讼，并走上法庭，向英国最有权势的官员提出了挑战。虽然这种行为并不出人意料，但接下来发生的事情震惊了英国的当权者，尤其是政府本身：法院做出了支持威尔克斯的裁决。法庭的裁决事实上推翻了国王及其手下几个世纪以来行使的权力，要求当局在进行搜查时需要依据更充分的理由，并且即使在拥有充分理由时，也要对其所作所为加以更多限制。英国媒体对这一裁决表示欢迎，并引用了一句著名的话——每个英国人的“家都是他的城堡，不容随意搜查，而他的文书也不容国王的信使在恶毒好奇心的驱使下随意偷窥”[注]。

就重要性而言，约翰·威尔克斯的诉讼标志着现代隐私权的诞生。这些权利受到所有自由人民的羡慕，包括生活在北美大陆的英国殖民者。就在1761年，他们曾在新英格兰为同样的争议而努力过，但最终输掉了官司。当时，年仅二十多岁的约翰·亚当斯还未成为一名律师，他坐在波士顿法庭的后排，见证了美洲大陆18世纪60年代初最伟大的一场法庭对决。小詹姆斯·奥蒂斯是马萨诸塞州最富战斗力的律师之一，他用和威尔克斯类似的理由抗议英国军队滥用权力。由于当地商人认为赋税不合法，他们选择走私进口货物以逃税，而英国人则回应以所谓通用搜查令，在没有具体证据的情况下挨家挨户搜查，以寻找违反海关规定的行为[注]。

奥蒂斯辩称，这是对公民自由的根本性侵犯，他称之为“滥用专断权力的至暗时刻”[注]。尽管奥蒂斯最终败诉，但他的话标志着北美殖民地人民迈

出了反抗的第一步。直至生命的最后时刻，亚当斯仍然记得奥蒂斯的论点，并写道，“他为这个国家注入了生命的气息”[注]。亚当斯表示，他至死都认为就是在那一天，那件案子，那个法庭，以及那个事件，标志着美国开始走向独立[注]。

直至13年后《独立宣言》发表，奥蒂斯热情倡导的原则才得以实现。那时，这个议题已经移师纽约，在那里，第一届美国国会于1789年在华尔街集会，詹姆斯·麦迪逊站在众议院面前，介绍了他提出的《权利法案》[注]。该法案包括成为美国宪法第四修正案的内容，保障了美国人的“人身、住宅、文件和财产”不受政府“无理搜查和扣押”的权利，包括使用“通用搜查令”采取上述行为[注]。自此之后，当局如果希望搜查任何住宅或办公室，则必须首先向一位独立法官提出申请，并提交“合理的理由”以获得搜查令。实际上，这意味着政府必须向法官证明，确实存在会导致拥有合理“理性的人”认为犯罪行为正在发生的事实[注]。

不过，这种保护是否应扩展到已经离开你家的信息？本杰明·富兰克林发明了邮局之后，第四修正案经受了考验。设想你仔细封好一个信封，并将其交由一个政府运营的机构邮寄，而19世纪的最高法院毫无争议地认定，人们针对其密封的信件仍然享有隐私权[注]。因此，第四修正案适用，政府不能在没有基于“合理理由”获得搜查令的情况下拆开信封检查信件内容，即使那封信是由政府邮局所保管的。

几个世纪以来，法院一直在审视人们是否有“合理的隐私期望”，并考虑将自己的信息存储于他人之处到底意味着什么。简而言之，如果这些东西放在一个上锁的储物箱中，而其他人无法拿到钥匙，那么法官将得出人们拥有类似期望的结论，因而第四修正案将适用。但是，如果你把你的文件放在一个文件盒中，并将其堆放在别人的文件盒旁边，而人们在那里自由来往，那么警察将不需要搜查令，因为法院认为，根据第四修正案，你已经放弃了对隐私的合理期望[注]。

由此看来，今天受到多重物理和数字安全措施严密保护的数据中心，显然完全符合上锁的储物箱的定义。

2013年夏，我们因斯诺登的事不断被一个又一个记者追逐，他们寻求着我们对某份最新泄露的机密文件的回应。一个司空见惯的场景经常出现，只要看到多米尼克又挤在约翰的办公室里密谈，我就知道又会有一篇报道即将发表。大多数时候，我们甚至不知道自己在回应什么。多米尼克回忆说：“在最初的几周里，我几乎每天都会和不同的记者进行同样的谈话。

他们会说，‘好吧，多米尼克，有人在撒谎，要么是微软，要么是爱德华·斯诺登’。”

《卫报》关于“棱镜”计划的报道只涉及更大事件的一部分，即美国国家安全局试图从私营企业获取数据的行为。正如现在已被泄密的文件详尽阐明的那样（注），2001年“9·11”悲剧发生后，美国国家安全局开始寻求与私营部门建立自愿合作关系，超出合法许可和授权范围搜集数据。

数据之惑

与其他领先的科技公司一样，微软也在纠结是否自愿向政府提供这些数据。我们就这些问题进行了内部讨论，并且清楚地意识到更广泛的地缘政治气候。“9·11”恐怖袭击的巨大阴影笼罩着整个国家。联军在阿富汗发动了“持久自由行动”，国会对入侵伊拉克表示了支持，心存恐惧的美国公众呼吁加强反恐努力。那是一个非常时期。正如许多人所说，它要求我们做出前所未有的非常反应。

但是，要求公司自愿提供泄密报告中所描述的那一类信息存在一个根本问题。美国国家安全局寻求的数据并不属于科技公司，而是属于客户，并且它们包含客户一些最私密的信息。

与“棱镜”计划一样，美国国家安全局在“9·11”事件后依照自愿原则从私营部门获取客户信息的努力也对我们提出了一个根本问题：“我们如何在履行保护国家义务的同时，履行我们对客户的责任？”

对我来说，答案很清楚。这个问题应该由法律解决。美国是一个法治国家，如果美国政府希望获得我们客户的记录，它需要遵守属地法律，得到法庭的批准。如果行政部门的官员们认为法律不够完备，他们可以通过国会寻求更多的权力。这是一个它应有的运行方式。

尽管在2002年，我们无法预测到爱德华·斯诺登和他的著名逃亡，但我们可以通过回望历史更精准地预测未来可能会发生什么。在国家面临危机之时，牺牲个人自由以换取国家安全并不是什么新鲜事。

美国宪法签署十多年后，国家就第一次面临这样的危机。1798年，美国和法国在加勒比海爆发了一场“准战争”。法国希望迫使美国偿还由当时已被推翻的法国国王提供的贷款，于是扣押了300多艘美国商船，并要求美国支付赎金（注）。部分愤怒的美国公众呼吁发动彻底的战争，但其他一些人，比如约翰·亚当斯总统，认为新生国家尚无力与法国抗衡。亚当斯担心公开辩论会对政府造成致命的伤害，于是他试图通过签署相关的4项法律

来平息这种不和谐，这4项法律被称为《外侨和煽动叛乱法》。这些法律允许政府监禁和驱逐“危险”的外国人，并使批评政府成为一种犯罪行为注。

大约60年后，在内战期间，美国再次暂时搁置了我们民主的一个关键原则：亚伯拉罕·林肯总统曾多次中止人身保护令，以镇压南方叛乱。为了加强征兵，林肯扩大了中止范围，并在全国范围内否决了审判权。在战争期间，有15000多名美国人未经法庭审判就被关进了监狱注。

1942年，日军轰炸珍珠港后不久，迫于军方和公众舆论的压力，富兰克林·罗斯福总统签署了一项行政命令，强迫12万日裔美国人进入地处偏远的集中营，营地被铁丝网包围，并由武装警卫看管。遭受监禁的人中有2/3出生在美国。该命令三年后才被撤销，当时遭到关押的大多数人已经失去他们的家园、企业和社区注。

尽管美国人民在国家危急时刻接受了这些不公正，但他们在后来开始质疑他们为公共安全付出的代价。我认为我们需要扪心自问的一个问题是：“从现在起再过10年，当危机过去后，我们将如何被评判。我们是否能说我们履行了对客户的承诺。”

如果问题很清楚，那么答案也显而易见。不经合法有效的法律程序，我们不能够自愿移交客户的数据。作为公司职位最高的律师，我必须履行我的职责，并承担因此而出现的任何批评。毕竟，有谁能比律师更好地捍卫我们所服务的客户的权利呢？

在这样的背景下，2013年夏，几乎所有领先的科技公司都发现自己处于防御状态，我们向政府官员表达了我们的挫败感。这成为一个转折点，标志着政府和企业的不同立场开始公开化，而这导致了两者之间至今仍然存在的巨大分歧。政府的职责是为居住在特定地区（如州或国家）的选民提供服务，但科技已经走向全球，我们的客户几乎遍布全世界。

云不仅改变了我们提供服务的地点和对象，还重新定义了我们与客户的关系。因为云的出现，科技公司在某些方面已经转变为类似银行的机构。人们把钱存进银行，而将他们最私人的信息——电子邮件、照片、文件和短信——存储在科技公司。

这种新型关系的影响已超出科技行业本身。正如20世纪30年代政府官员们认为，银行对经济实在过于重要，因此必须受到监管一样，今天的科技公司已变得太过重要，因而不能再延续当前的放任政策。科技公司需要受到更积极的法律法规监管。但与20世纪30年代的银行不同，如今的科技公司

在全球范围内运营，这使得整个监管问题更加复杂。

2013年，随着全球客户的不满情绪不断加剧，我们意识到，要想缓解他们的担心，我们必须更加公开。我们对自己遵循的准则十分清楚，无论是针对我们自身提供服务的清晰限制，还是针对后来收购公司的某些既有做法所实施的复杂处理。我们希望向客户解释，我们只有在收到搜查令、法院传票和国家安全命令时才会向相关部门移交客户信息。但当我们提议面向大众公开沟通这一信息时，美国司法部告诉我们，上述内容属于保密信息，我们不能公开。我们对此深感沮丧。

我们决定做一件从未做过的事情——起诉美国政府。作为一家公司，我们曾经和政府打了10年反垄断官司，然后又花了10年的时间努力达成和解，现在这么做无异于破釜沉舟，背水一战。我们最初向外国情报监控法庭（FISC）提出了一项保密动议。

FISC是一个特别法庭，专门审查政府的监控命令。它创建于冷战期间，目的是批准窃听、电子数据收集以及监视可疑的恐怖分子和间谍。它非常神秘，以保护情报部门监控和挫败安全威胁的努力。根据《外国情报监视法》签发的每一份搜查令都附有一份封口令，禁止我们告知客户我们已经收到了针对他们数据的搜查令。虽然这一点可以理解，但我们的法律诉求是，根据宪法第一修正案及其对言论自由的承诺，我们有权与公众分享更多的信息。我们辩称，我们至少应有权笼统地公开我们所收到命令的数量和类型。

很快，我们了解到谷歌也采取了同样的行动。这成为另一个转折点。5年来，我们两家公司一直在全球各地的监管机构面前激烈斗争，提出不同的主张。谷歌主张对Windows操作系统进行限制，而微软主张限制谷歌搜索。我们对彼此了然于胸。我非常尊敬谷歌的总法律顾问肯特·沃克，虽然没有人会认为我们是好朋友。

突然，我们站在了同一条战壕，共同与我们自己的政府展开了一场全新的战斗。我决定主动和肯特取得联系，但在开始时并没有什么进展，只是交换了几条信息。7月的一个早晨，结束了在Xbox团队所在的大楼内举行的一次员工大会后，我掏出手机准备再试一次。我想找一个安静的角落，然后发现自己站在一个真人大小的士官长纸板剪影前——他是我们制作的游戏《光环》中的人物，带领军队对抗外星敌人的士兵。我很高兴能够背靠这位士官长打这通电话。

肯特接了电话。我们以前曾交谈过很多次，但几乎总是在讨论双方公司之间的相互投诉。现在我提出了一个不一样的建议：“让我们携起手来，看看是否能共同与司法部进行谈判。”

就算肯特怀疑我的提议是特洛伊木马，我也不会责怪他。但他认真听取了我的提议，并且在第二天联系我，同意进行合作。

我们与政府举行了一次联合会议，试图达成共同的条款。就在8月底，眼看就达成协议时，谈判突然以失败告终。从我们的角度来看，似乎美国国家安全局和联邦调查局的立场并不相同。随着2013年的夏去秋来，斯诺登持续披露的内容进一步加深了美国政府和科技行业之间的隔阂，形势也变得越来越糟。

10月30日，《华盛顿邮报》发表了一篇令整个行业抓狂的报道：“斯诺登的文件显示，美国国家安全局入侵了雅虎和谷歌全球数据中心的链接。”[注]这篇报道的作者之一是巴特·盖尔曼，他是我十分尊重的一位记者，我们是普林斯顿大学的同学，我在他还在为《普林斯顿人日报》撰稿的时候就已经认识他。他在文章中说，在英国政府的帮助下，美国国家安全局正在秘密利用海底光缆从雅虎和谷歌的网络中复制数据。虽然我们无法证实美国国家安全局是否也已经盯上我们的光缆，但斯诺登的一些文件确实提到了我们用户的电子邮件和信息服务[注]。这让我们怀疑，我们也受到了监听。直至今日，美国和英国政府都还没有公开否认过非法入侵数据光缆的指控。

面对这个消息，科技行业既惊又怒。在某种程度上，这篇报道填补了缺失的一环，从而解开了我们对斯诺登文件的一些困惑。它表明，美国国家安全局拥有的数据要比我们按照国家安全命令和搜查令合法提供的数据多得多。如果这是真的，政府实际上是在大规模地搜查和扣押公民的私人信息。

《华盛顿邮报》的报道表明，美国国家安全局与英国的有关部门合作，从美国科技公司使用的光缆中截获数据，并且可能没有经过司法审查或监督。我们担心这种行为发生在英国光缆交叉的地方。在行业内的律师们交换了各自的信息后，我们认为，美国国家安全局说服自己，通过与英国政府合作或依赖英国政府，并且在美国境外采取行动，它就可以不受美国宪法第四修正案约束，因而国家安全局搜查和扣押信息的行为不再必须遵循正当程序和法庭命令。

微软和整个行业迅速做出反应。在接下来的几周里，我们和其他公司宣布，将对通过光缆在数据中心之间传输的所有数据以及存储在数据中心服务器上的数据实施严格的加密[注]。这是保护客户隐私的一个根本性步骤。因为这意味着，即使政府通过监听光缆获取了客户数据，也几乎肯定无法解锁和读取。

此类加密技术提升看似容易，但实际实现起来很困难。它涉及我们的数据中心要进行大量计算工作，并需要做大量的工程工作。我们工程团队的一些负责人对此并不积极，并且他们的担心是可以理解的。考虑到在可行的时间线内，能够应用的工程资源有限，软件开发从本质上说总是需要在不同特性上做出取舍。因此，新增的加密工作需求会导致他们推迟开发其他产品功能，而这些功能是客户要求我们添加的。经过激烈的讨论，首席执行官史蒂夫·鲍尔默和我们的高管团队做出决定，必须快速推进加密领域的工作。其他科技公司也都采取了相同行动。

未来，枪口将会调转

当年11月，在这些事件不断发酵的背景下，奥巴马总统来西雅图出席一个政治筹款活动。在正式活动后，白宫邀请了一小群地区领袖和支持者，在西雅图威斯汀酒店举办了一个鸡尾酒会。我应邀代表微软参加了活动。

我希望在这次活动中能有几分钟时间和总统谈谈我们在诉讼中提出的和宪法第一修正案有关的问题，但是司法部的律师事先要求我们不要和总统提起与诉讼相关的事宜。“他们的客户”由律师代表，因而所有谈话都必须经过律师进行。不过，就在奥巴马总统抵达会议室之前，我询问他的助手瓦莱丽·贾勒特，向总统提出一个与我们的诉讼无关的问题是否合适，即他是否认为第四修正案对美国人免受政府不合理搜查和扣押的保护同样适用于美国境外。

鉴于《华盛顿邮报》的报道内容，即美国国家安全局窃听美国公司在美国境外运营的光缆，我认为这是一个重要的问题。瓦莱丽认为总统会觉得这个话题很有趣。

她猜得没错。我和总统一谈起这个话题，他立刻变回了以前宪法学教授的模样。奥巴马总统对宪法的掌握显然远超于我，不过，我也勉力回忆起足够多的内容，撑起了一次还算专业的谈话。

然后，总统改变了话题。

“我听说你们都不想与我们和解，因为你们觉得让大家看到你们正在起诉政府会更好。是这样的吗？”这是一个关键时刻，需要迅速在心里权衡利弊做出快速反应。司法部的律师显然从未指示我们不能直接回答美国总统的问题，于是我坦率地回答了他的问题，解释说我们想解决诉讼，但政府似乎并不愿意。我阐述了我们的担忧并坦陈，我相信如果我们把恰当的人聚在同一间屋里，我们就能取得真正的进展。

几周后，奥巴马邀请一些科技行业的领袖到白宫做客。当时距离圣诞节只

有8天，白宫西翼已经为节日装扮一新，一派忙碌的景象。在总统去夏威夷度假前，员工们全力以赴地结束手头的工作。白宫已经公开宣布，此次会议将讨论“健康、IT（信息技术）采购和监听问题”。这有点像告诉棒球迷们，他们将参加一个活动，议程包括唱国歌、吃热狗比赛和观看世界大赛的开场比赛。我们都清楚地知道，在那个寒冷的冬日早晨把我们带到华盛顿来的是什么。

当天来到白宫西翼的可谓科技界的全明星阵容，包括苹果首席执行官蒂姆·库克、谷歌董事长埃里克·施密特、脸书首席运营官谢丽尔·桑德伯格、网飞首席执行官里德·黑斯廷斯以及其他十多位业界领袖。我们中的大多数人早已相互认识，其中8家公司——几乎是行业内所有竞争对手——刚刚聚在一起建立了一个新的联盟，叫作“改革政府监听”，其目的正是合作解决我们当天要讨论的问题。经过一轮热情的寒暄，我们将自己的智能手机放进走廊的一排小柜子内，然后鱼贯进入罗斯福厅。

罗斯福厅并不是因为一位总统而得名，而是因为两位总统而得名，即西奥多·罗斯福和富兰克林·罗斯福，前者建造了白宫西翼，后者对其进行了扩建[注]。我在长长的抛光会议桌旁坐下，一抬头便看到一幅挂在壁炉顶上的画，并不禁笑了一声。那幅画中的人物是“泰迪”身为“莽骑兵”骑在马上的硬汉形象[注]。我希望接下来的90分钟不会那么硬碰硬。

白宫方面同样派出最强阵容迎接我们。奥巴马总统和副总统乔·拜登照例坐在了中间，他们两侧分坐着几乎所有的高级官员。在记者团拍照时，总统和里德聊了聊下一季的《纸牌屋》，并问了几个无伤大雅的安全问题。

媒体离开房间后，谈话开始进入正题。奥巴马总统执政期间，此类会面的惯例是首先让每位客人发表自己的意见。考虑到当天参加会面的人数，这颇花费了一些时间。总统祭出他苏格拉底式的提问技巧，把对谈话要点的复述逐步变成一场深入的对话。

除了少数几个人之外，其他每位科技行业的领袖都强烈主张限制大规模数据搜集，提高透明度，并对国家安全局的行为进行更多监察和平衡。我们在会面的大部分时间内避免直接谈论爱德华·斯诺登这个话题。但是，随着谈话的进行，坐在奥巴马身边的社交游戏公司Zynga的创始人马克·平卡斯辩称，斯诺登是一位英雄。“您应该赦免他，”平卡斯表示，“并为他举行一场盛大的欢迎仪式。”[注]

拜登明显不安地扭动了一下身体，而奥巴马总统则回答说：“我绝对不会这样做。”他解释说，斯诺登偷偷携带众多文件逃离美国，他认为这是不负责任的行为。

接下来轮到坐在平卡斯旁边的雅虎首席执行官玛丽莎·梅耶尔发言。她打开一个厚厚的纸质文件夹，取出精心准备的谈话要点，并说道："我同意大家所说的一切。"随后，她停下来抬头看了看，指着平卡斯说："除了他之外，我不同意他的话。"所有人都笑了起来。

上面的对话反映出我们都想勉力达成一种平衡。几乎所有人来白宫都是为了敦促总统改变政府的做法，但科技行业与奥巴马一直维持着友好，甚至是热诚的关系，就像在去一个人家里做客时，你总是不好挑战主人，尤其他还是白宫的主人。

尽管我们都极其礼貌，但我们仍然坚持自己的立场，提出政府必须改革监听机制。很明显，奥巴马认真地思考了整个议题，阐明了他认为政府需要解决的一系列问题。他有时会以退为进地表示，虽然公众对国家安全局掌握的那些数据感到担心，但如果把在座公司手中掌握的数据加起来，则比政府所掌握的多得多。他说："我怀疑，未来枪口将会调转。"

当会面结束时，总统明确表示，他有意对美国政策进行一些重要（尽管有限）的改变。他滔滔不绝地谈到一些问题，并要求人们提供更多的信息，以帮助谈话"进入后续的落实层面"。

一个月后，2014年1月17日，总统就政府监听改革迈出了第一步注。在他公布计划的前一天晚上，我们接到了司法部律师的电话。他们希望就微软和谷歌提起的诉讼达成和解，开出的条款比我们在8月谈判中所要求的更加优惠。和解达成之后，科技公司立即推出了新的透明度报告，公布了更多关于国家安全搜查令和命令的数据。这要归功于谷歌，它行动最快，为我们树立了一个令人印象深刻的榜样，其他公司决定效仿。

对于许多客户和隐私权的倡导者来说，奥巴马的讲话仅仅是一个开始，政府仍有许多需要改革之处。在整个科技行业，我们都赞同这一观点。我们认识到，这个问题并不容易，要解决它仍存在重重困难。我们如何才能让外国政府和客户放心，美国政府不会不适当地进入由美国公司运营的数据中心？我们怎样才能同时采取必要的合法步骤来保障公众的安全？这些问题需要很多年才能解决。

从斯诺登7个月前将偷来的文件交给《卫报》以来，形势已经发生了如此大的转变，这一切真是不可思议。人们开始关注政府监听的范围，更强大的加密措施也已成为新的标准，科技公司起诉了它们自己的政府，而竞争对手以新的方式展开了合作。

几年后，人们仍在争论爱德华·斯诺登到底是英雄还是叛国者。在一些人眼中，他两者兼具。但是到2014年初，有两点毋庸置疑——他已经改变了世

界，也已经改变了整个科技行业。

---

1. Glenn Greenwald, “NSA Collecting Phone Records of Millions of Verizon Customers Daily,” *Guardian*, June 6,2013, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

2. Glenn Greenwald and EwenMacAskill, “NSA Prism Program Taps In to User Data of Apple, Google and Others,” *Guardian*, June 7,2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

3. Benjamin Dreyfuss and Emily Dreyfuss, “What Is the NSA’s PRISM Program?(FAQ),” *CNET*, June 7,2013, https://www.cnet.com/news/what-is-the-nsasprism-program-faq/.

4. 时任美国国家情报总监的詹姆斯·克拉珀后来将该计划描述为“一个政府内部计算机系统，用于协助政府在法律授权和法院监督下，从电子通信服务提供商处收集外国情报信息”。Robert O’Harrow Jr., Ellen Nakashima and Barton Gellman, “U.S., Company Officials: Internet Surveillance Does Not Indiscriminately Mine Data,” *Washington Post*, June 8,2013, https://www.washingtonpost.com/world/national-security/us-company-officials-internetsurveillance-does-not-indiscriminately-mine-data/2013/06/08/5b3bb234d07d-11e2-9f1a-1a7cdee20287_story.html?utm_term＝.b5761610edb1。

5. Glenn Greenwald,EwenMacAskill,and Laura Poitras, “Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations,” *Guardian*,June 11,2013, https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsawhistleblower-surveillance.

6. Michael B. Kelley, “NSA: Snowden Stole 1.7 Million Classified Documents and Still Has Access to Most of Them,” *Business Insider*, December 13, 2013, https://www.businessinsider.com/how-many-docs-did-snowdentake-2013-12.

7. Ken Dilanian,Richard A. Serrano, and Michael A. Memoli, “Snowden Smuggled Out Data on Thumb Drive, Officials Say,” *Los Angeles Times*,June 13, 2013,http://articles.latimes.com/2013/jun/13/nation/la-

na-nsaleaks-20130614.

8. Nick Hopkins, “UK Gathering Secret Intelligence Via Covert NSA Operation,”*Guardian*,June 7,2013, https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism；see also MirrenGidda, “Edward Snowden and the NSA Files——Timeline,” *Guardian,*August 21，2013，https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline.

9. William J. Cuddihy, The Fourth Amendment: Origins and Meaning, 1602–1791 (Oxford: Oxford University Press, 2009), 441.

10. William J. Cuddihy, The Fourth Amendment: Origins and Meaning, 1602–1791 (Oxford: Oxford University Press, 2009),442。

11. William J. Cuddihy, The Fourth Amendment: Origins and Meaning, 1602–1791 (Oxford: Oxford University Press, 2009),459。

12. Frederick S. Lane, American Privacy: The 400-Year History of Our Most Contested Right (Boston: Beacon Press, 2009), 11.

13. David Fellman, The Defendant’s Rights Today (Madison: University of Wisconsin Press, 1976)，258.

14. William Tudor, The Life of James Otis, of Massachusetts: Containing Also,Notices of Some Contemporary Characters and Events, From the Year 1760 to 1775 (Boston: Wells and Lilly, 1823)，87–88。在美国的开国元勋于1776年7月2日在费城投票支持独立后第二天，亚当斯回忆起奥蒂斯的言论对马萨诸塞州人民的巨大影响。亚当斯早早醒来，给自己的妻子阿比盖尔写了一封信，并追忆了奥蒂斯的重要地位。Brad Smith, “Remembering the Third of July,”Microsoft on the Issues (blog), Microsoft, July 3, 2014, https://blogs.microsoft.com/on-the-issues/2014/07/03/remembering-the-third-of-july/。

15. David McCullough, *John Adams* (New York: Simon & Schuster, 2001), 62.William Cranch, *Memoir of the Life, Character, and Writings of John Adams* (Washington, DC: Columbian Institute, 1827), 15。有趣的是，奥蒂斯的倡导和亚当斯对其重要性的认识，至今仍一直影响着美国的公共政策和法律。美国首席大法官约翰·罗伯茨在2014年首次引用了他们的话，当时他代表做出一致裁定的最高法院书写了意见，要求执法部门在检查嫌疑人智能手机的内容之前获得搜查令。*Riley v. California*, 573 U.S._(2014),

https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf，27–28。罗伯茨于2018年重申了这一立场，当时他代表最高法院多数法官书写意见称，警方同样需要搜查令才可以获取手机的位置信息记录。*Carpenter v. United States*, No. 16-402, 585 U.S.(2017), https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf，5。

16. Thomas K, Clancy, The Fourth Amendment: Its History and Interpretation(Durham, NC: Carolina Academic Press, 2014), 69–74.

17. 美国宪法第四修正案。

18. Brent E. Turvey and Stan Crowder, Ethical Justice: Applied Issues for Criminal Justice Students and Professionals (Oxford: Academic Press, 2013),182–83.

19. Ex parte Jackson, 96 U.S. 727 (1878).

20. Cliff Roberson, Constitutional Law and Criminal Justice, second edition(BocaRaton, FL: CRC Press, 2016), 50; Clancy, The Fourth Amendment,91–104.

21. Charlie Savage, “Government Releases Once-Secret Report on Post-9/11 Surveillance,” *New York Times*, April 24, 2015，https://www.nytimes.com/interactive/2015/04/25/us/25stellarwind-ig-report.html.

22. Terri Diane Halperin, The Alien and Sedition Acts of 1798: Testing the Constitution (Baltimore: John Hopkins University Press, 2016), 42–43.

23. Terri Diane Halperin, The Alien and Sedition Acts of 1798: Testing the Constitution (Baltimore: John Hopkins University Press, 2016),59–60。

24. David Greenberg, “Lincoln’s Crackdown,” *Slate*,November 30, 2001，https://slate.com/news-and-politics/2001/11/lincoln-s-suspension-of-habeas-corpus.html.

25. T. A. Frail, “The Injustice of Japanese-American Internment Camps Resonates Strongly to This Day,” Smithsonian, January 2017，https://www.smithsonianmag.com/history/injustice-japanese-americans-internmentcamps-resonates-strongly-180961422/.

26. Barton Gellman and AshkanSoltani, “NSA Infiltrates Links to Yahoo,Google Data Centers Worldwide, Snowden Documents Say,” *Washington Post,* October 30, 2013，https://www.washingtonpost.com/world/nationalsecurity/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwidesnowden-documents-say/2013/10/30/e51d661 e-4166-11e3-8b74d89d714ca4dd_story.html?noredirect＝on&utm_term＝.5c2f99fcc376.

27. “Evidence of Microsoft’s Vulnerability,” *Washington Post,* November 26,2013，https://www.washingtonpost.com/apps/g/page/world/evidence-ofmicrosofts-vulnerability/621/.

28. Craig Timberg, Barton Gellman and Ashkan Soltani, “Microsoft, Suspecting NSA Spying, to Ramp Up Efforts to Encrypt Its Internet Traffic,” *Washington Post*, November 26, 2013，https://www.washingtonpost.com/business/technology/microsoft-suspecting-nsa-spying-to-ramp-up-efforts-to-encryptits-internet-traffic/2013/11/26/44236b48-56a9-11e3-8304-caf30787c0a9_story.html?utm_term＝.69201c4e9ed8.

29. “Roosevelt Room,” White House Museum，accessed February 20, 2019，http://www.whitehousemuseum.org/west-wing/roosevelt-room.htm.

30. “泰迪”（Teddy）是西奥多·罗斯福的昵称，“莽骑兵”为美国前总统西奥多·罗斯福于1898年美西战争期间组织的一支志愿骑兵团。——译者注

31. 几篇新闻报道集中报道了平卡斯向奥巴马提出的赦免斯诺登的建议。SethRosenblatt, “ ‘Pardon Snowden,’ One Tech ExecTells Obama, Report Says,”*Cnet*，December 18, 2013, https:// www.cnet.com/news/pardon-snowdenone-tech-exec-tells-obama-report-says/；Dean Takahashi, “Zynga’s Mark Pincus Asked Obama to Pardon NSA Leaker Edward Snowden,” *Venture Beat,* 2013年12月18日，https://venturebeat.com/2013/12/19/zyngas-markpincus-asked-president-obama-to-pardon-nsa-leaker-edward-snowden/。

32. “Transcript of President Obama’s Jan. 17 Speech on NSA Reform,”*Washington Post*，January 17, 2014，https://www.washingtonpost. com/politics/full-text-of-president-obamas-jan-17-

speech-on-nsareforms/2014/01/17/
fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html?
utm_term=.c8d2871c4f72.

This Chapter is not free

This Chapter is not free

This Chapter is not free

This Chapter is not free

This Chapter is not free

This Chapter is not free

This Chapter is not free